

BAB I

PENDAHULUAN

1.1. Latar Belakang Masalah

Beberapa tahun terakhir terjadi perkembangan yang sangat pesat di dunia teknologi komunikasi. Salah satunya terjadi pada perangkat telepon selular (ponsel). Ponsel memiliki banyak sekali fasilitas yang disediakan dan salah satunya adalah *Short Message Service* (SMS) yang berfungsi untuk melakukan pengiriman data berupa pesan teks dari suatu perangkat ponsel ke perangkat ponsel lain. Namun fasilitas SMS ini masih memiliki beberapa kekurangan yaitu mengenai keamanan pesan yang akan dikirim.

Pesan yang akan dikirim perlu dijaga kerahasiaannya agar hanya pengirim dan penerima pesan yang mengetahui isinya. Untuk itu diperlukan suatu teknik untuk mengamankan pesan yang akan dikirim yaitu menggunakan kriptografi.

Kriptografi adalah ilmu yang berguna untuk mengacak (kata yang lebih tepat adalah masking) data sedemikian rupa sehingga tidak bisa dibaca oleh pihak ketiga. Tentu saja data yang diacak harus bisa dikembalikan ke bentuk semula oleh pihak yang berwenang.

Oleh karena itu, muncul suatu gagasan untuk membangun aplikasi pengamanan menggunakan kombinasi metode *Base 64*, *Shift Cipher* Dan *XOR* agar dihasilkan algoritma yang kuat, dan selanjutnya pesan sms terenkripsi tersebut akan dikompresi sebelum dikirim.

1.2. Rumusan Masalah

Melihat dari latar belakang yang telah dianalisa maka dirumuskan permasalahan yaitu, bagaimana membuat sebuah aplikasi pengamanan data SMS menggunakan Metode kriptografi dengan Algoritma *Base 64*, *Shift Cipher* dan *XOR* kemudian pesan SMS dikompresi dengan Metode *Huffman*.

1.3. Ruang Lingkup

Mengingat luasnya permasalahan yang timbul maka diperlukan batasan untuk menghindari meluasnya masalah dalam pembahasan, yaitu :

1. Pengamanan data pada enkripsi dimulai menggunakan kombinasi metode *Base 64*, *Shift Cipher* dan *XOR*, sebaliknya pada dekripsi dimulai menggunakan kombinasi metode *XOR*, *Shift Cipher* dan *Base 64*.

2. Basis bilangan yang digunakan adalah tabel ASCII 128 dan *Base 64*.
3. Algoritma kompresi yang digunakan adalah metode *Huffman*.
4. Ponsel yang digunakan mendukung teknologi *Java* dengan MIDP 2.0 dan CLDC 1.1.

1.4. Tujuan

Tujuan dari penelitian ini adalah membangun sebuah aplikasi pengaman SMS berbasis J2ME menggunakan kombinasi metode *Base 64*, *Shift Cipher* dan *XOR* sehingga selain pemilik hp tidak dapat mengetahui isi pesan yang tersandikan.

Aplikasi ini diharapkan juga dapat bermanfaat untuk mengkompresi data tanpa merusak isi data tersebut.